

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
11 July 2002 (11.07.2002)

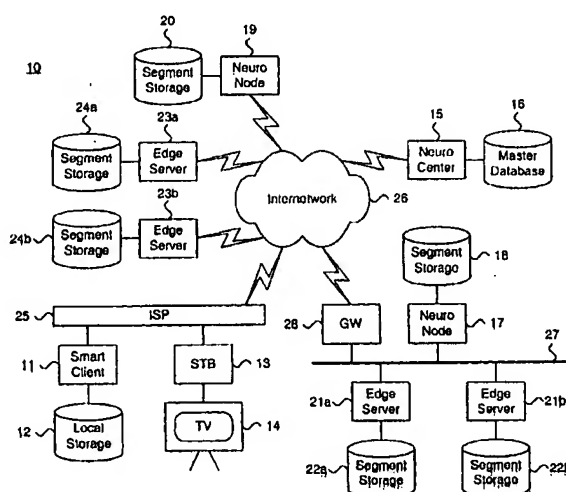
PCT

(10) International Publication Number
WO 02/054708 A2

- (51) International Patent Classification⁷: H04L 29/06, 9/00, G06F 17/30, H04L 12/18
- (74) Agent: INOUE, Patrick; 810 Third Avenue, Suite 258, Seattle, WA 98104 (US).
- (21) International Application Number: PCT/US02/00332
- (22) International Filing Date: 2 January 2002 (02.01.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/259,503 2 January 2001 (02.01.2001) US
60/262,529 17 January 2001 (17.01.2001) US
- (71) Applicant (for all designated States except US): TRANZ-SEND BROADCASTING NETWORK, INC. [US/US]; 601 Van Ness, Suite E3444, San Francisco, CA 94102 (US).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): REDMOND, Scott, D. [US/US]; 601 Van Ness Avenue, Suite E3613, San Francisco, CA 94012 (US).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- Published:
— without international search report and to be republished upon receipt of that report

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PROVIDING LOAD BALANCED SECURE MEDIA CONTENT AND DATA DELIVERY IN A DISTRIBUTED COMPUTED ENVIRONMENT



(57) Abstract: A system and method for providing load balanced secure media content and data delivery (10) in a distributed computing environment is disclosed. Media content is segmented and encrypted into a set of individual encrypted segments on a centralized control center (15). Each individual encrypted segment has the same fixed size. The complete set of individual encrypted segments is staged to a plurality of intermediate control nodes (17, 19). Individual encrypted segments are mirrored from the staged complete set to a plurality of intermediate servers (21a-b, 23a-b). Requests are received from clients (11) for the media content at the centralized control center. Each individual encrypted segment in the set is received from one of an intermediate control node and an intermediate server optimally sited from the requesting client. The individual encrypted segments are reassembled into the media content for media playback.

WO 02/054708 A2



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR PROVIDING LOAD BALANCED SECURE MEDIA**5 CONTENT AND DATA DELIVERY IN A DISTRIBUTED COMPUTING****ENVIRONMENT**

This patent application is a conversion of U.S. provisional patent applications, Serial No. 60/259,503, filed January 2, 2001, pending; and Serial No. 60/262,529, filed January 17, 2001, pending; the priority dates of which are claimed pursuant to 35 U.S.C. §119(e) and the
10 disclosures of which are incorporated by reference.

TECHNICAL FIELD

The present invention relates in general to media content delivery and, in particular, to a system and method for providing load balanced secure media content delivery in a distributed computing environment.

15 BACKGROUND OF THE INVENTION

Television is the most widely available form of mass audiovisual communications in use today. The basic format of television is relatively mature, consisting primarily of television network-operated transmission stations sending programming signals to passive receivers or "sets." Media content, in the form of television shows and advertising, are transmitted over
20 specific radio frequencies and program selection is limited to the programming broadcast at any given time.

Cable- and satellite-based television network services offer an alternative to conventional radio frequency-based television programming. Both formats offer superior reception quality and provide an extensive selection of media content by airing a wider range of television
25 channels. Of late, these network services have begun to offer "pay-per-view" programming services. Using set-top boxes, subscribers can purchase time-restricted access to view content made available on controlled television channels. Popular content includes first run movies and sporting events. Although more flexible than conventional television, "pay-per-view" formats only provide access to the additional content aired by the cable or satellite networks at specific
30 show times on standard television sets and are not broadcast via other means.

Recognizing this shortfall, media content providers operating over internetworks, and specifically, the Internet, have begun to offer downloadable media content as an alternative to television broadcast programming. Live media content is aired as streaming media and static, pre-recorded media content is staged on content servers for retrieval and playback by clients on
35 demand. Television, as well as radio, programming is also available. To view media content

over an internetwork, users use a Web browser to navigate to the desired media content and then execute a media playback application within the Web browser to download and view the selected shows and other content.

Although more customizable than standard television programming, Internet-based
5 "media-on-demand" (henceforth, simply "media-on-demand") services suffer from numerous shortcomings. The most apparent shortcoming is a drastic difference in viewing experience. Personal computer displays offer a higher resolution than standard NTSC television sets. This difference negatively effects the appearance of media content. Moreover, Web browser-based media playback applications display media at low resolutions in small viewing windows with
10 low fidelity sound, thereby further degrading the viewing experience.

As well, media-on-demand is network infrastructure-sensitive. Media content is generally downloaded as a series of streamed serialized packets. To improve throughput, the loss of individual packets can be tolerated to a certain degree at the expense of distortion during playback. However, media content delivery is contingent on the continued availability of the
15 content server and is subject to bandwidth and network load constraints. As well, delivery is further limited by the processing capability of each client.

In addition, most media content is subject to copyright and other forms of digital rights protections. However, media content is often staged with little or no privilege or access safeguards. Content is freely available for downloading and viewing without significant copying
20 or distribution protections. Once downloaded, redistribution consequently becomes uncontrollable and infringements virtually impossible to police.

Similarly, media-on-demand further lacks electronic commerce (e-commerce) and electronic business (e-business) support. E-commerce concerns conducting on-line transactions over an internetwork and e-business concerns running a business based on a network-centric
25 business model. However, users generally request media from a content server with minimal interaction. With few exceptions, no transaction processing, order management, or advertising and product targeting take place. Media content is simply downloaded and viewed with potential business opportunities lost.

In the prior art, direct download and media content streaming are the two predominant
30 forms of media content retrieval. Direct download involves the retrieval of media content from a content server *en masse*. The user browses available data files containing media content and downloads a media content selection in the same way as any other file. This approach is slow and inefficient, as content is unicast from the content server to the requesting client in a one-to-one connection. Furthermore, less bandwidth-capable clients suffer further, as most content
35 servers are architected to service the fastest connections first.

Media content streaming involves the delivery of media content in a series of individual packets at a data rate preferably exceeding the rate of consumption. Individual packets are received in serial order and stored in a temporary buffer until the requesting client has received packets sufficient to enable playback. However, streaming is bandwidth-dependent and also
5 unicast.

Therefore, there is a need for an approach to delivering full-function, full-motion media-on-demand in a distributed computing environment. Preferably, such an approach would provide secure reliable content delivery through a hierarchical media service infrastructure.

There is a further need for an approach to serving media content via a distributed network
10 framework incorporating fault tolerance and dynamic load balancing. Preferably, such an approach would offer content provider support functions including user profiling and e-commerce and e-business management.

DISCLOSURE OF INVENTION

The present invention provides a system and method for delivering encrypted segmented
15 media content to individual clients through a dynamically load balanced network framework. Media content is encoded to a uniform format and is segmented and encrypted, preferably using one unique key per segment. A centralized control center, known as a Neuro Center, stages complete sets of the segmented encrypted media content to intermediate control nodes, known as Neuro Nodes, dispersed throughout the network. The Neuro Nodes then mirror select individual
20 encrypted segments to intermediate servers, known as Edge Servers, and, in a further embodiment, to individual clients, known as Smart Clients. The Edge Servers and Smart Clients maintain the mirrored individual encrypted segments for eventual delivery to requesting Smart Clients. Via a client, a user requests delivery of media content from the centralized control center, which validates the request and furnishes a validation certificate enabling delivery of the
25 requested content. The client then requests each individual encrypted segment from either an intermediate control node, intermediate server, or, in a further embodiment, a peer client, on a segment-by-segment basis, based on network load and component availability. Playback of the delivered media content begins upon the receipt of sufficient individual encrypted segments.

An embodiment of the invention provides a system and method for providing load
30 balanced secure media content delivery in a distributed computing environment. Media content is segmented and encrypted into a set of individual encrypted segments on a centralized control center. Each individual encrypted segment has a same fixed size. The complete set of individual encrypted segments is staged to a plurality of intermediate control nodes. Individual encrypted segments are mirrored from the staged complete set to a plurality of intermediate servers.
35 Requests are received from clients for the media content at the centralized control center. Each

individual encrypted segment in the set is received from one of an intermediate control node and an intermediate server optimally sited from the requesting client. The individual encrypted segments are reassembled into the media content for media playback. The segments may be received from different servers in non-sequential order. The requesting client should acquire the
5 first segment from whichever of the intermediate control node or intermediate server that can deliver the first segment fastest, thus providing an immediate-playback start capability.

Still other embodiments of the present invention will become readily apparent to those skilled in the art from the following detailed description, wherein is described embodiments of the invention by way of illustrating the best mode contemplated for carrying out the invention.
10 As will be realized, the invention is capable of other and different embodiments and its several details are capable of modifications in various obvious respects, all without departing from the spirit and the scope of the present invention. Accordingly, the drawings and detailed description are to be regarded as illustrative in nature and not as restrictive.

DESCRIPTION OF THE DRAWINGS

15 FIGURE 1 is a block diagram showing a system for providing load balanced secure media content delivery in a distributed computing environment.

FIGURE 2 is a process flow diagram showing load balanced secure media content delivery via the system of FIGURE 1.

FIGURE 3 is a process flow diagram showing load balanced secure media content
20 delivery with peer-to-peer intercommunication in accordance with a further embodiment.

FIGURE 4 is a process flow diagram showing load balanced secure media content delivery with pre-casted media content staging in accordance with a further embodiment.

FIGURE 5 is a block diagram showing the software modules of the Neuro Center of FIGURE 1.

25 FIGURE 6 is a block diagram showing the software modules of a Neuro Node of FIGURE 1.

FIGURE 7 is a block diagram showing the software modules of an Edge Server of FIGURE 1.

FIGURE 8 is a block diagram showing the software modules of a Smart Client of
30 FIGURE 1.

FIGURE 9 is a data structure diagram showing a play ticket used by the system of FIGURE 1.

FIGURE 10 is a data structure diagram showing a validation certificate used by the system of FIGURE 1.

FIGURE 11 is a data structure diagram showing a packet header used by the system of FIGURE 1.

FIGURE 12 is a flow diagram showing a method for providing load balanced secure media content delivery in a distributed computing environment.

5 FIGURE 13 is a flow diagram showing a routine for performing the operations of the Neuro Center for use in the method of FIGURE 12.

FIGURE 14 is a flow diagram showing a routine for performing the operations of a Neuro Node for use in the method of FIGURE 12.

10 FIGURE 15 is a flow diagram showing a routine for performing the operations of an Edge Server for use in the method of FIGURE 12.

FIGURE 16 is a flow diagram showing a routine for performing the operations of a Smart Client for use in the method of FIGURE 12.

BEST MODE FOR CARRYING OUT THE INVENTION

15 FIGURE 1 is a block diagram showing a system 10 for providing load balanced secure media content delivery in a distributed computing environment. Media content is delivered as individual encrypted segments to a Smart Client 11 or, alternatively, to a set-top box (STV) 13 for airing on a television set (TV) 14. The Smart Client 11 provides media viewing playback capabilities to personal computers, wireless devices, public display kiosks, and the like. The Smart Client 11 includes a local storage 12 in which the segments are transitorily stored.

20 Henceforth, for clarity of discussion, media content delivery will be described with reference to the Smart Client 11 only, although one skilled in the art would recognize that a similar form of delivery would apply to a set-top box 13 or similar media access device. The Smart Client 11 is further described below with reference to FIGURE 8.

 The Smart Client 11 initiates the media content delivery process by sending a request to a

25 Neuro Center 15. The Neuro Center 15 centrally manages all requests for media content and is accessible via an internetwork 26, including the Internet, or similar broadband wide area network. The Smart Client 11 interfaces to the internetwork 26 through an Internet Service Provider 25 (ISP) or via direct connection (not shown). The Neuro Center 15 maintains a master database 16 in which individual users are profiled and e-commerce and e-business management

30 data are maintained. Upon validating each client request, the Neuro Center 15 requests the Smart Client 11 to check the network and commence media content delivery. The Neuro Center 15 is further described below with reference to FIGURE 5.

 The actual media content is stored as individual encrypted segments on Neuro Nodes 17 and 19 and Edge Servers 21a-b and 23a-b. Neuro Node 17 and Edge Servers 21a-b are locally

35 interfaced via an intranetwork 27 and are interfaced to the Neuro Center 15 via a gateway (GW)

28 interfacing to the internetwork 26. Neuro Node 19 and Edge Server 23a-b directly interface to the Neuro Center 15 via the internetwork 26. Other configurations and network topologies are feasible, as would be recognized by one skilled in the art.

5 The Neuro Nodes 17 and 19 maintain segment storages 18 and 20, respectively, in which complete sets of individual encrypted segments comprising a complete (or portion of a) media selection are stored. The Edge Servers 21a-b and 23a-b also maintain segment storages 22a-b and 24a-b, respectively, in which mirrored segments are maintained. The Neuro Nodes 18 and 19 selectively copy or "mirror" segments to the Edge Servers 21a-b and 23a-b to optimally balance the distribution of individual encrypted segments throughout the network. Neural Nodes
10 17 and 19 are further described below with reference to FIGURE 6 and Edge Servers 21a-b and 23a-b are further described below with reference to FIGURE 7.

The individual computer systems, including Neuro Center 15, Neuro Nodes 17 and 19, Edge Servers 21a-b, and 23a-b, and Smart Client 11, are general purpose, programmed digital computing devices consisting of a central processing unit (CPU), random access memory
15 (RAM), non-volatile secondary storage, such as a hard drive or CD ROM drive, network interfaces, and peripheral devices, including user interfacing means, such as a keyboard and display. Program code, including software programs and data, are loaded into the RAM for execution and processing by the CPU and results are generated for display, output, transmittal, or storage.

20 FIGURE 2 is a process flow diagram showing load balanced secure media content delivery 40 via the system of FIGURE 1. The key to achieving dynamic load balancing is through the continuous determination of network throughput and load characteristics using client-generated "pulses". A pulse is generated prior to requesting each individual encrypted segment to identify an optimally sited Neuro Node or Edge Server from which to request the
25 segment. Media content delivery begins with a Smart Client 41 sending a request 45 to a Neuro Center 42 (step ①). In response, the Neuro Center 42 validates the client request 45 and sends a response 46 requesting the Smart Client to "pulse" the network status prior to commencing delivery (step ②).

The requested media content is delivered in individual encrypted segments received from
30 Neuro Nodes 43 and Edge Servers 44. Prior to receiving each segment, Smart Client 41 broadcasts a "pulse" 47 over the network to determine the load and operational status of the various Neuro Nodes 43 and Edge Servers 44 (step ③). The Smart Client 41 receives "pulse" responses and segments 48 back from the Neuro Nodes 43 and Edge Servers 44 (step ④). The Neuro Center 42 manages encryption and security in the background to media content delivery.

The "pulse" responses indicate the network load and relative status of each network component while each segment contains a portion of the actual requested media content. The Smart Client 41 reassembles the individual encrypted segments and begins media playback upon receiving a sufficient number of segments. The Smart Client 41 decrypts and decompresses each segment and provides a full-featured, full-motion playback. Note the segments need not be received in serial order and can be (and in practice, often are) requested from different Neuro Nodes 43 and Edge Servers 44, depending on network load and component status.

FIGURE 3 is a process flow diagram showing load balanced secure media content delivery with peer-to-peer intercommunication 60 in accordance with a further embodiment.

The Smart Client 61 takes advantage of media content already made available on peer Smart Client 65 through peer-to-peer segment sharing. This approach improves file delivery capabilities and provides a highly scalable network with a rich intermediate content server population.

As before, a Smart Client 61 sends a request 66 to a Neuro Center 62 to initiate media content delivery (step ①). The Neuro Center 62 validates the request and sends a response 67 requesting the Smart Client 61 to "pulse" the network (step ②). The Smart Client 61 broadcasts a "pulse" 68 over the network to the Neuro Nodes 63, Edge Server 64 and other Smart Clients 65 (step ③). These components send back responses and segments 69 (step ④) as above.

FIGURE 4 is a process flow diagram showing load balanced secure media content delivery with pre-casted media content staging 80 in accordance with a further embodiment. Ordinarily, a Neuro Center 81 is only initially involved in media content delivery during the validation of individual user requests. However, to substantially minimize the delay attendant to media content delivery during peak demand times, the Neuro Center 81 can pre-cast 84 (step ①) media content to each Smart Client 82 during off-peak times. The initial segments of popular media content are thereby staged at individual Smart Clients 82 for immediate playback by a user without incurring a delay due to network load and demand. Once playback begins, the remaining segments are sent to each Smart Client 82 in a continuous multicast 85 from the Neuro Center 81 (step ②).

FIGURE 5 is a block diagram showing the software modules 100 of the Neuro Center 101 of FIGURE 1. The Neuro Center 101 functions as a centralized control center and is primarily responsible for preparing raw media content 112 for distribution as individual encrypted segments 115 and for validating individual user requests. The Neuro Center 101 includes eight modules: encoding 102, segmentation 103, encryption 104, profiling and e-commerce 105, request processing 106, ticket validation 107, pre-casting 108, and multicasting and broadcasting 109.

The encoding module 102 receives raw media content 112 from a variety of diverse sources, including the Internet, satellite and cable feeds, wireless devices, and next-generation media sources. The raw media content 112 is converted into a standardized form of encoded content 114. In turn, the segmentation module 103 segments the encoded content 114 into sets of individual segments 115 which are then encrypted by the encryption module 104, preferable using a different unique key for each individual segment. The complete sets of individual encrypted segments 115 are then broadcast by the multicasting and broadcasting module 109 to the Neuro Nodes (shown in FIGURE 1) for mirroring to Edge Servers and, in a further embodiment, Smart Clients.

Individual users request media content delivery by sending a play ticket 110, as further described below with reference to FIGURE 9. The play ticket 110 identifies the user and requested media content. The request processing module 106 processes each request and the ticket validation module 107 validates the play ticket 110. The ticket validation module 107 accesses a ticket database 118 to validate the play ticket 110 and generate a validation certificate 111 which is sent back to the requesting client. The profiling and e-commerce module 105 accesses user profiles 116 and e-commerce data 117 to provide demographics tracking and order management. As well, advertising and product targeting can be delivered via the profiling and e-commerce module 105.

The pre-casting module 108 is used in a further embedment to stage the initial segments of popular media content to the individual Smart Clients during off-peak times. Finally, the multicasting and broadcasting module 109 sends sets of segments 115, as well as individual encrypted segments, to a select subset of network components (multicasting) or to all network components (broadcasting).

FIGURE 6 is a block diagram showing the software modules 120 of a Neuro Node 121 of FIGURE 1. Each Neuro Node 121 functions as an intermediate control node within the network. The Neuro Center (shown in FIGURE 1) sends complete sets of individual encrypted segments, collectively constituting a complete work, to each Neuro Node 121 for staging and mirroring. Each Neuro Node 121 includes four modules: mirroring 122, request processing 123, multicasting and broadcasting 124, and codec 125.

The mirroring module 122 selectively stages individual encrypted segments 128 to Edge Servers and, in a further embodiment, Smart Clients. The segments are distributed throughout the network to maximize load balancing and fault tolerance. The request processing module 123 receives incoming requests from individual Smart Client. The requests are staged in a request queue 126. The multicasting and broadcasting module 123 sends a requested segment 128 if the Neuro Node 121 is optimally sited relative to the requesting Smart Client. Alternatively, a

plurality of individual client requests for the same segment 128 can be stored in the request queue 126 and fulfilled *en masse* by the multicasting and broadcasting module 124. The advantage of staging multiple client requests is network throughput efficiency. The request processing module 123 authenticates each user through a user authentication table 129. The
5 Neuro Node 121 monitors the network status 127 in the background. The codec 125 compresses individual encrypted segments 128 prior to delivery to a Smart Client.

FIGURE 7 is a block diagram showing the software modules 140 of an Edge Server 141 of FIGURE 1. Each Edge Server 141 functions as an intermediate server within the network. The Neuro Nodes (shown in FIGURE 1) mirror select individual encrypted segments to each
10 Edge Server 141 for staging. Each Edge Server 141 includes four modules: request processing 142, segment receipt 143, multicasting and broadcasting 144, and codec 145. The segment receipt module 142 receives individual encrypted mirrored segments 148 selectively staged by the Neuro Nodes.

The request processing module 142 receives incoming requests from individual Smart
15 Clients. The requests are staged in a request queue 146. The Edge Server 141 sends a mirrored requested segment 148 if the Edge Server 141 is optimally sited relative to the requesting Smart Client. Alternatively, a plurality of individual client requests for the same mirrored segment 148 can be stored in the request queue 146 and fulfilled *en masse* by the multicasting and broadcasting module 144. The advantage of staging multiple client requests is network
20 throughput efficiency. The request processing module 142 authenticates each user through a user authentication table 149. The Edge Server 141 monitors the network status 147 in the background.

FIGURE 8 is a block diagram showing the software modules 160 of a Smart Client 161 of FIGURE 1. Each Smart Client 161 initiates, facilitates and delivers media content to a
25 requesting user. The Smart Client 161 includes six modules: user interface 162, request processing 163, segment receipt 164, multicasting and broadcasting 165, codec 166, and playback 167.

The user interface 162 provides controls to select media content for delivery. The request processing module 163 forms a request for media content that is sent to the Neuro Center (shown
30 in FIGURE 1) to initiate content delivery. The segment receipt module 164 receives individual downloaded segments 168 from the Neuro Nodes, Edge Servers, and, in a further embodiment, Smart Clients. A "pulse" is sent over the network via the multicasting and broadcasting module 165 to determine the current status of the network. The segment receipt module 164 also receives pre-cast segments 169 sent by the Neuro Center during off-peak times. Similarly, the
35 segment receipt module 164 stages mirrored segments 170 received from Neuro Nodes when

providing peer-to-peer intercommunications, in accordance with a further embodiment. The codec 166 decompresses the individual downloaded segments 168 and pre-cast segments 169. The codec 166 performs decryption of each individual segment including the decryption by a unique key through use of the play ticket 110 and validation certificate 111 (both shown in
5 FIGURE 5). Finally, the playback module 167 provides full-feature playback functionality, including play, pause, stop, rewind, fast forward, full screen, chapter stops, shuttle bar, and similar features.

Each module in the Neuro Center 101, Neuro Node 120, Edge Server 140, and Smart Client 160 is a computer program, procedure or module written as source code in a conventional
10 programming language, such as the C++ programming language, and is presented for execution by the CPU as object or byte code, as is known in the art. The various implementations of the source code and object and byte codes can be held on a computer-readable storage medium or embodied on a transmission medium in a carrier wave. The system operates in accordance with a sequence of process steps, as further described below with reference to FIGURE 12.

15 FIGURE 9 is a data structure diagram showing a play ticket 180 used by the system 10 of FIGURE 1. Each play ticket 180 is used to transact the purchase or rental of delivered media content. Briefly, a play ticket 180 is issued on an individual customer basis and contains information about the movie ordered. Only a portion of the movie key for each movie is stored on a play ticket 180 to disable decryption and safeguard against theft and unauthorized access.
20 The movie key also prevents reuse of the play ticket 180.

When a customer orders media content from a Neuro Center (shown in FIGURE 1), a play ticket 180 is generated and includes the following:

- (1) Certificate serial number for the ticket (181);
- (2) Customer number (182);
- 25 (3) Creation date and time (183);
- (4) Expiration date and time (184);
- (5) Movie title number (185);
- (6) Number of plays (186)
- (7) Movie key (Part 1) (188); and
- 30 (8) Certificate signature (189).

The Certificate signature 189 is a digital signature prepared using symmetric public key encryption. The certificate signature 189 ensures the ticket cannot be altered without validation. As well, the movie key part 1 188 includes only a portion of the entire movie key, which is split into two pieces between the play ticket 180 and a validation certificate 200 (shown below in
35 FIGURE 10).

In the described embodiment, each play ticket 180 has a 96-byte structure containing all information necessary to validate the play ticket. The certificate serial number 181 is used as a record lookup key into the ticket database 118 (shown in FIGURE 5). The customer number 182 and movie title number 185 are also stored in the ticket database 118 and validated when the play ticket is used.

Before the play ticket 180 is presented for validation by the Neuro Center, the Smart Client checks the certificate signature 189 for validity. The certificate signature 189 includes a checksum of the certificate consisting of the first 64 bytes which are cryptographically signed using the Digital Signature Standard (DSS). If the play ticket 180 has been altered, the certificate signature 189 will not match and the signature validation will fail.

The number of plays field 186 can contain either a special numeric value indicating the ticket is good for unlimited plays, that is, the user has purchased the media content, or a numeric value indicating the number of plays remaining in a rental of the media content. Unlimited play tickets 180 do not have an expiration date and time 184.

Generally, all other play tickets 180 are good for only one play. If the number of plays in the play ticket 180 is greater than one, the play ticket 180 must be replaced. When validated, a replacement play ticket 180 is also returned with the number of plays field 186 reduced and a new certificate serial number 181 issued.

FIGURE 10 is a data structure diagram showing a validation certificate 200 used by the system 10 of FIGURE 1. Each validation certificate 200 includes essentially the same information as a play ticket 180 as follows:

- (1) Certificate serial number for the validation certificate (201);
- (2) Customer number (202);
- (3) Creation date and time (203);
- (4) Expiration date and time (204);
- (5) Movie title number (205);
- (6) Reserved (206);
- (7) Movie key (Part 2) (207); and
- (8) Certificate signature (208).

Like the play ticket 180, the Neuro Node validates each validation certificate 200 using the certificate signature 208. If the certificate signature 208 does not match, the validation certificate 200 is invalid. The validation certificate 200 includes the other remaining portion of the movie key Part 2 207.

In the described embodiment, each movie key is split into two parts by using a second 128-bit random number generated using the same operations as used to generated the movie key

Part 1. The second 128-bit random number is used as a split filter using an exclusive OR operation against the full movie key. The value used to split the key becomes the validation key.

Play tickets are computed according to the following operation:

$$K_2 = K_M \oplus K_1$$

5 where:

K_M is the Movie Key

K_1 is the Validation Key (Split Value)

K_2 is the Play Ticket Key

The validation key is stored in the ticket database 118, along with the other information
10 necessary to validate the play ticket 180. The play ticket key becomes part of the play ticket 180.

During the later validation phase, after the play ticket information has been validated against the ticket database 118, a validation certificate 200 is generated and sent to the user. This certificate includes the validation key. The full movie key is recovered by using an exclusive OR of the two values to reverse the split process and recover the original key.

15 FIGURE 11 is a data structure diagram showing a packet header 220 used by the system 10 of FIGURE 1. A packet header 220 is prepended to each segment to enable a Smart Client (shown in FIGURE 1) to reassemble the media content and enable playback. In the described embodiment, the individual data packets are sent in accordance with the Tranz-Cast Delivery Protocol (TCDP), a data exchange network based on the Reliable Multicast Framework (RMF).

20 The fixed header of each TCDP data packet contains the following fields:

- (1) Sources (221): port number from which the packet was sent;
- (2) Destination (222): port number to which the packet was directed;
- (3) Packet Length (223): contains a count of octets in the packet, including the header and data;
- 25 (4) Checksum (224): corresponds to the Internet protocol checksum;
- (5) Type (225): identifies the type of packet;
- (6) Data Owner (226): contains a unique identifier for the originator of the data.
Together with the sequence number, the contents of this field uniquely define a packet when multiple senders share a common multicast address;
- 30 (7) Sequence Number (227): increments by one for each new packet sent and may be used by the receiver to detect packet loss and to restore packet sequence;
- (8) Header Extensions (228): indicates the presence of a header extension field; and
- (9) Data (229): Variable payload data is appended to the end of the header 220 and may be of any length, including zero, as specified by the type field.

Other types and combinations of fields are possible, as would be recognized by one skilled in the art.

FIGURE 12 is a flow diagram showing a method for providing load balanced secure media content delivery 240 in a distributed computing environment. Each of the individual components, the Neuro Center, Neuro Nodes, Edge Servers, and Smart Clients, operate independently following initialization and start-up (blocks 241-244, respectively). With the exception of the Neuro Center, the various components can initiate and terminate their respective processing asynchronously without significantly affecting the continued operation of the remaining components. Following initialization and start-up, the method completes.

FIGURE 13 is a flow diagram showing a routine for performing the operations of the Neuro Center 250 for use in the method of FIGURE 12. The purpose of this routine is to initially, and as necessary, stage complete segment sets to Neuro Nodes for mirroring and validate individual user requests.

Thus, complete sets of segments 115 (shown in FIGURE 5) are sent to Neuro Nodes. Thereafter, user requests are processed in an iterative processing loop (block 252-263) as follows. During each iteration (block 252), a user request is received (block 253) from a Smart Client and the corresponding user profile 116 is looked up (block 254). The play ticket 180 (shown in FIGURE 9) is looked up in the ticket database 118 (block 255) and, if valid (block 256), a validation certificate 200 (shown in FIGURE 10) is generated (block 258). If more plays are left on the play ticket 180 (block 259), a replacement play ticket 180 is generated (block 260). The validation certificate 200 and a replacement play ticket 180 are sent to the user (block 261) and the e-commerce data 117 is updated (block 262).

If the play ticket 180 is not valid (block 256), an invalid play ticket message is sent to the user (block 257) and the e-commerce data is updated (block 262). Processing continues with each subsequent user request (block 263), after which the routine returns.

FIGURE 14 is a flow diagram showing a routine for performing the operations of a Neuro Node 270 for use in the method of FIGURE 12. The purpose of this routine is to mirror individual encrypted segments to the Neuro Nodes and to deliver requested segments to Smart Clients.

Thus, initially and as required thereafter, individual encrypted segments 128 (shown in FIGURE 6) are mirrored to Neuro Nodes and, in a further embodiment, to Smart Clients, for providing load balancing and optimal retrieval of media content over the network (block 271). User requests are then processed in an iterative processing loop (blocks 272-276) as follows. During each iteration (block 272), a user request is received (block 273) from a Smart Client. The requested segment 128 is retrieved (block 274) from the segment storage and sent to the

requesting user (block 275). Iterative processing continues (block 276) until the Neuro Node terminates, after which the routine returns.

FIGURE 15 is a flow diagram showing a routine for performing the operations of an Edge Server 280 for use in the method of FIGURE 12. The purpose of this routine is to receive individual encrypted mirrored segments and to deliver requested segments to Smart Clients.

Thus, initially and as required thereafter, individual encrypted segments are received from Neuro Nodes and staged as mirrored segments 148 (shown in FIGURE 7). User requests are then processed in an iterative processing loop (blocks 282-286) as follows. During each iteration (block 282), a user request is received (block 283) from a Smart Client. The requested segment 128 is retrieved (block 284) from the segment storage and sent to the requesting user (block 285). Iterative processing continues (block 286) until the Edge Server terminates, after which the routine returns.

FIGURE 16 is a flow diagram showing a routine for performing the operations of a Smart Client 290 for use in the method of FIGURE 12. The purpose of this routine is to request delivery of and playback media content selected by a user. In a further embodiment, the Smart Client provides peer-to-peer intercommunications by serving individual encrypted mirrored segments to other Smart Clients.

Thus, in a further embodiment, individual encrypted mirrored segments 170 (shown in FIGURE 8) are staged (block 291) for retrieval by peer Smart Clients. Thereafter, media content requests are processed in an iterative processing loop (blocks 292-306) as follows. During each iteration (block 292), media content is ordered (block 293) through the user interface 162. A play ticket 180 (shown in FIGURE 9) is received from the Neuro Center (block 294) and validated by the Smart Client (block 295) by authenticating the certificate signature 189. If the play ticket 180 is not valid (block 296), the media content is re-ordered (block 297) from the Neuro Center.

The status of the network is determined prior to requesting each individual segment (blocks 298-300) as follows. First, a "pulse" is sent from the Smart Client (block 298) to the Neuro Nodes, Edge Servers and, in a further embodiment, peer Smart Clients. A pulse report is received back from each of the components (block 299) and an optimal route is determined (block 300) for each of the individual encrypted segments.

Each individual encrypted segment is requested (block 301) and received (block 302), preferably from an optimally sited network component. If segments sufficient for playback have been received (block 303), playback begins (block 304). Receipt of segments continues (block 305) until media content delivery is complete. Processing media content requests continues (block 306) until the Smart Client terminates.

In a further embodiment, the Smart Client sends individual encrypted mirrored segments 170 to peer Smart Clients upon request (blocks 307-109) as follows. A user request for an individual encrypted segment is received (block 307). The requested mirrored segment 170 is retrieved (block 308) and sent to the requesting user (block 309). The delivery of mirrored segments 170 from a peer Smart Client enables fuller network resource utilization and improved load balancing characteristics for the network.

While the invention has been particularly shown and described as referenced to the embodiments thereof, those skilled in the art will understand that the foregoing and other changes in form and detail may be made therein without departing from the spirit and scope of the invention.

CLAIMS

1. A system for providing load balanced secure media content delivery (10) in a distributed computing environment, comprising:
- a centralized control center (15) segmenting and encrypting media content into a set of individual encrypted segments each having a same fixed size;
 - a plurality of intermediate control nodes (17, 19) staging the complete set of individual encrypted segments;
 - a plurality of intermediate servers (21a-b, 23a-b) mirroring individual encrypted segments from the staged complete set; and
 - a client (11) sending requests for the media content to the centralized control center, receiving each individual encrypted segment in the set from one of an intermediate control node and an intermediate server optimally sited from the requesting client, and reassembling the individual encrypted segments into the media content for media playback.
2. A system according to Claim 1, further comprising:
- a queue (126, 146) queuing requests from a plurality of clients on at least one of one such single intermediate control node and one such intermediate server; and
 - a multicasting module (124, 144) on the at least one of one such single intermediate control node and one such intermediate server multicasting the individual encrypted segments to the clients.
3. A system according to Claim 1, further comprising:
- an encryption module (104) encrypting each individual encrypted segment to a unique encryption key.
4. A system according to Claim 1, further comprising:
- a segmentation module (103) determining the fixed size for each individual encrypted segment based on a running time of the media content.
5. A system according to Claim 1, further comprising:
- a codec (166) executing at each requesting client to decode each individual encrypted segment.

6. A system according to Claim 1, wherein the centralized control center balances media content delivery between each intermediate control node and intermediate server.

7. A system according to Claim 1, further comprising:
5 a playback module (167) enabling media playback at each requesting client prior to receipt of substantially all individual encrypted segments.

8. A system according to Claim 1, further comprising:
a playback module (167) providing flexible media playback at each requesting client
10 comprising functions selected from the group comprising pause, rewind, fast-forward, skip forward, skip backward, chapter stops, and a shuttle bar.

9. A system according to Claim 1, further comprising:
a broadcasting module (155) broadcasting a pulse from each requesting client prior to
15 receiving each individual encrypted segment; and
a request processing module (163) selecting the optimally-sited one of intermediate control node and an intermediate server based on responses to the pulse.

10. A system according to Claim 1, further comprising:
20 a mirroring module (122) mirroring individual encrypted segments from the staged complete set to a plurality of peer clients; and
a request processing module (163) receiving each individual encrypted segment in the set from one of an intermediate control node, an intermediate server and a peer client optimally sited from the requesting client.

25

11. A system according to Claim 1, wherein the centralized control center staging individual encrypted segments comprising an initial portion of the media content to a plurality of clients and sending individual encrypted segments comprising a remaining portion of the media content to the plurality of clients upon request.
30

12. A method for providing load balanced secure media content delivery (240) in a distributed computing environment, comprising:
segmenting and encrypting (103, 104) media content into a set of individual encrypted segments each having a same fixed size on a centralized control center;

- staging (251) the complete set of individual encrypted segments to a plurality of intermediate control nodes;
- mirroring (281) individual encrypted segments from the staged complete set to a plurality of intermediate servers;
- 5 receiving (253) requests from clients for the media content at the centralized control center;
- receiving (302) each individual encrypted segment in the set from one of an intermediate control node and an intermediate server optimally sited from the requesting client; and
- reassembling (304) the individual encrypted segments into the media content for media
- 10 playback.
13. A method according to Claim 12, further comprising:
- queuing (273, 283) requests from a plurality of clients on at least one of one such single intermediate control node and one such intermediate server; and
- 15 multicasting (275, 285) the individual encrypted segments to the clients.
14. A method according to Claim 12, further comprising:
- encrypting (104) each individual encrypted segment to a unique encryption key.
- 20 15. A method according to Claim 12, further comprising:
- determining (103) the fixed size for each individual encrypted segment based on a running time of the media content.
16. A method according to Claim 12, further comprising:
- 25 executing (302) a codec at each requesting client to decode each individual encrypted segment.
17. A method according to Claim 12, further comprising:
- balancing (251) media content delivery between each intermediate control node and
- 30 intermediate server via the centralized control center.
18. A method according to Claim 12, further comprising:
- enabling (304) media playback at each requesting client prior to receipt of substantially all individual encrypted segments.
- 35

19. A method according to Claim 12, further comprising:
providing (304) flexible media playback at each requesting client comprising functions selected from the group comprising pause, rewind, fast-forward, skip forward, skip backward, chapter stops, and a shuttle bar.
- 5
20. A method according to Claim 12, further comprising:
broadcasting a (298) pulse from each requesting client prior to receiving each individual encrypted segment; and
selecting (300) the optimally-sited one of intermediate control node and an intermediate
10 server based on responses to the pulse.
21. A method according to Claim 12, further comprising:
mirroring (271) individual encrypted segments from the staged complete set to a plurality
of peer clients; and
15 receiving (302) each individual encrypted segment in the set from one of an intermediate control node, an intermediate server and a peer client optimally sited from the requesting client.
22. A method according to Claim 12, further comprising:
staging (108) individual encrypted segments comprising an initial portion of the media
20 content to a plurality of clients; and
sending (109) individual encrypted segments comprising a remaining portion of the media content to the plurality of clients upon request.
23. A computer-readable storage medium holding code for performing the method
25 according to Claims 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, or 22.

1/17

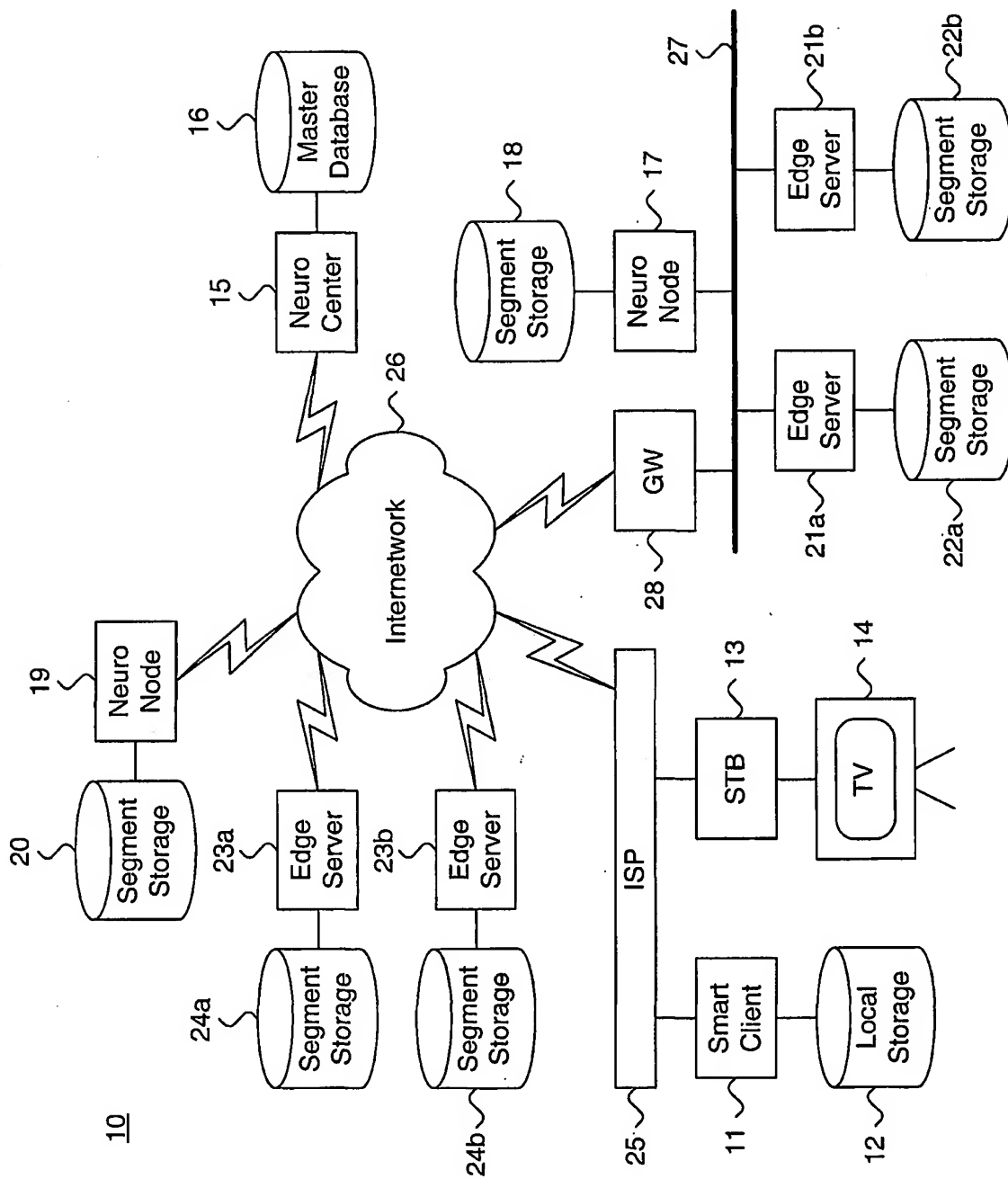
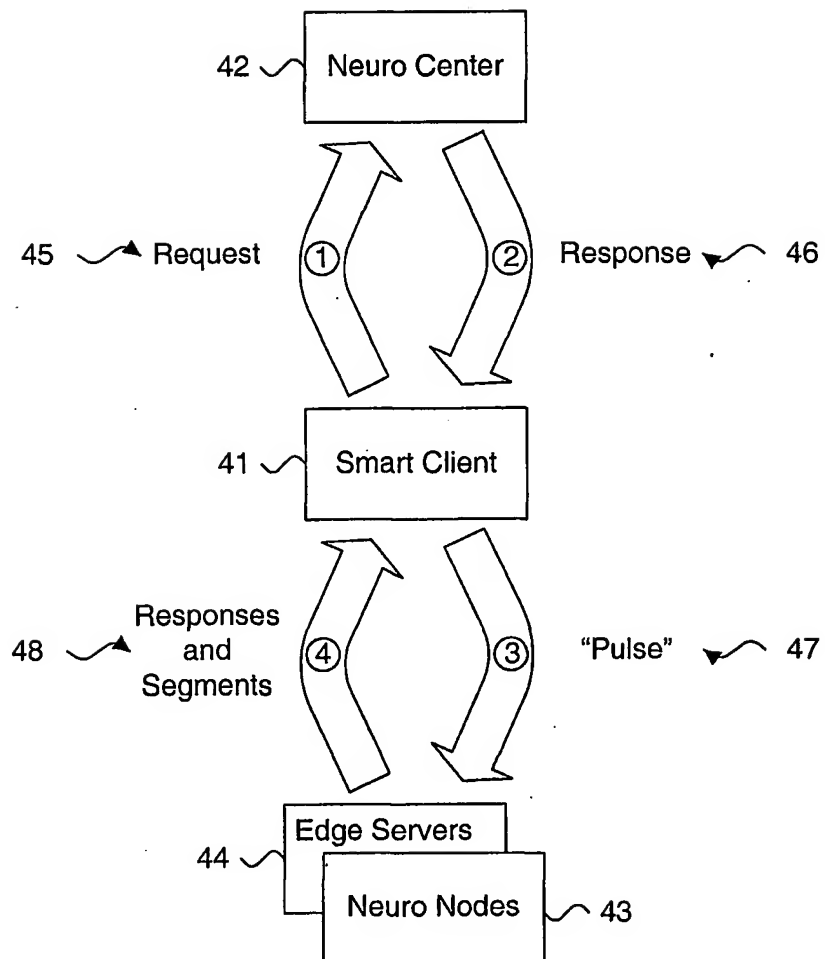


Figure 1.

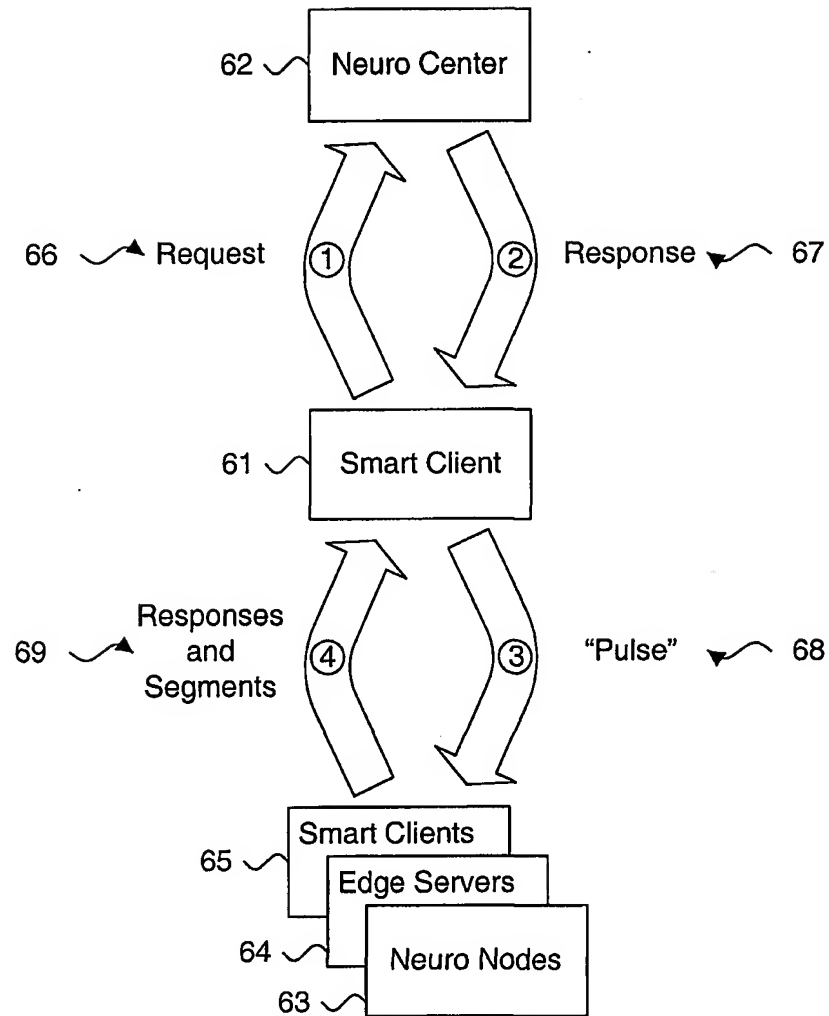
2/17

Figure 2.

40

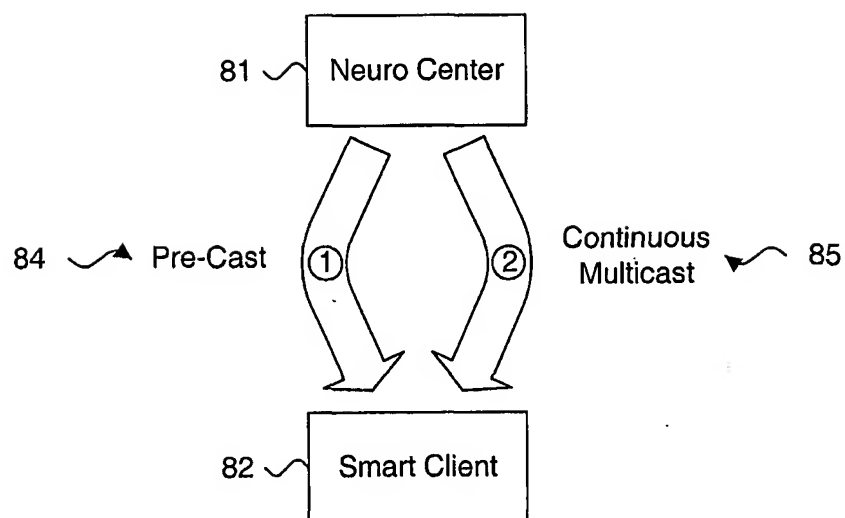
3/17

Figure 3.

60

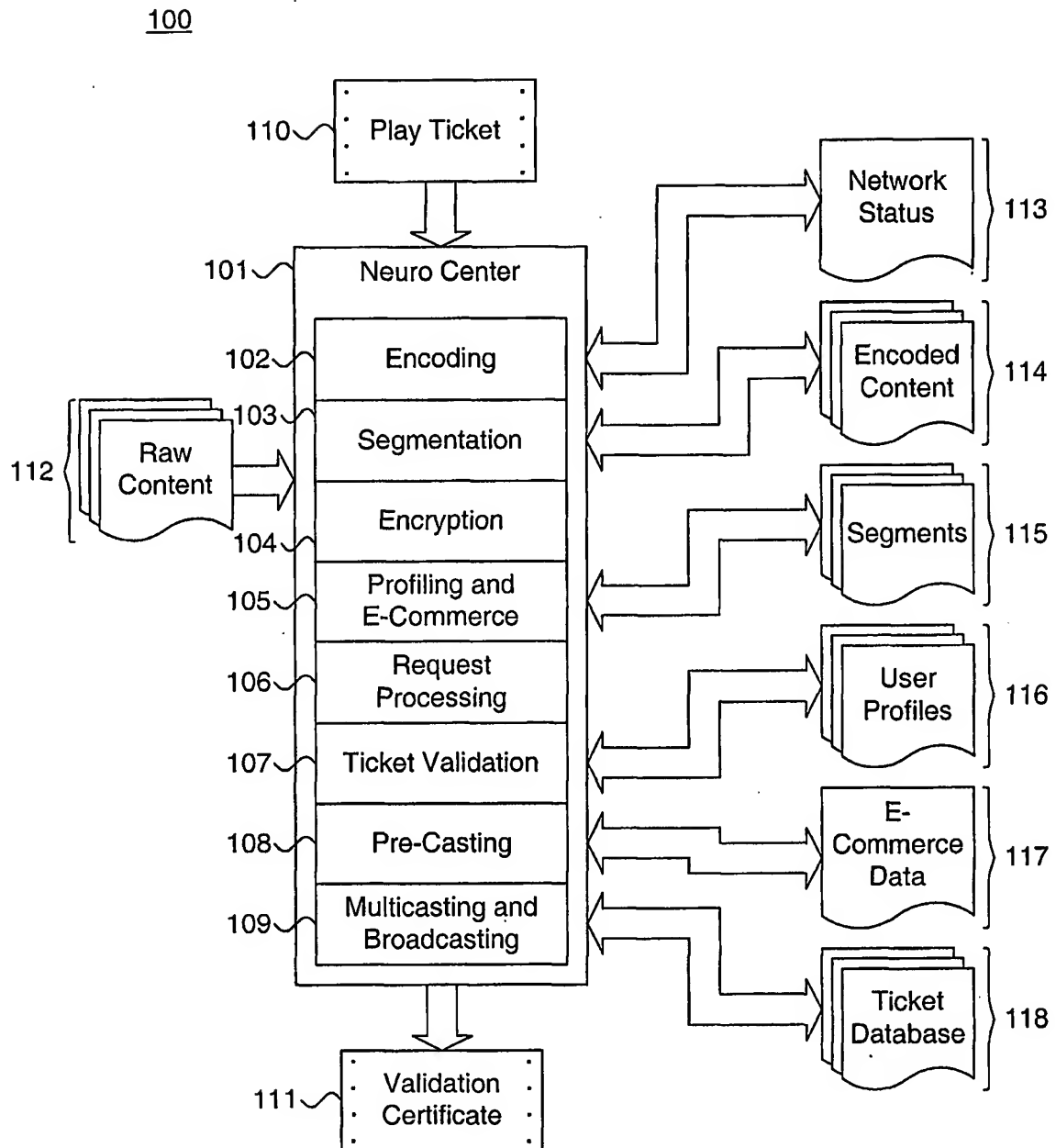
4/17

Figure 4.

80

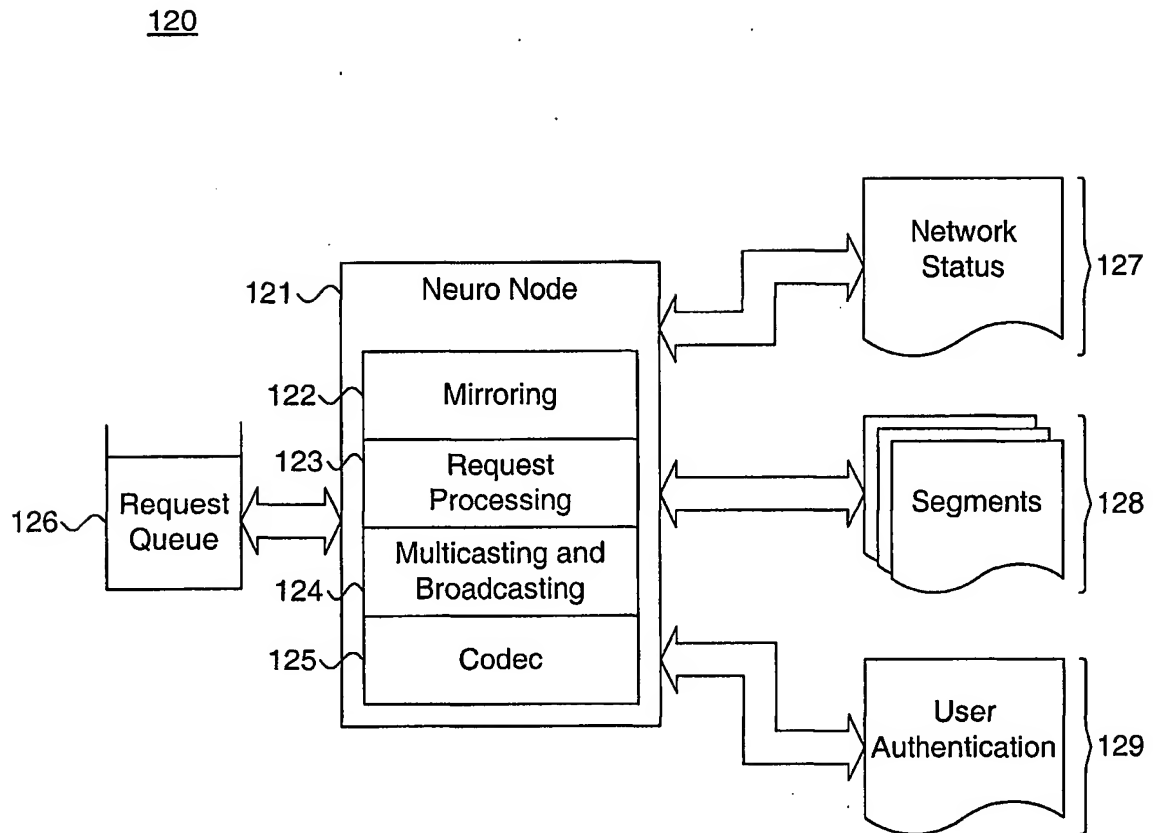
5/17

Figure 5.



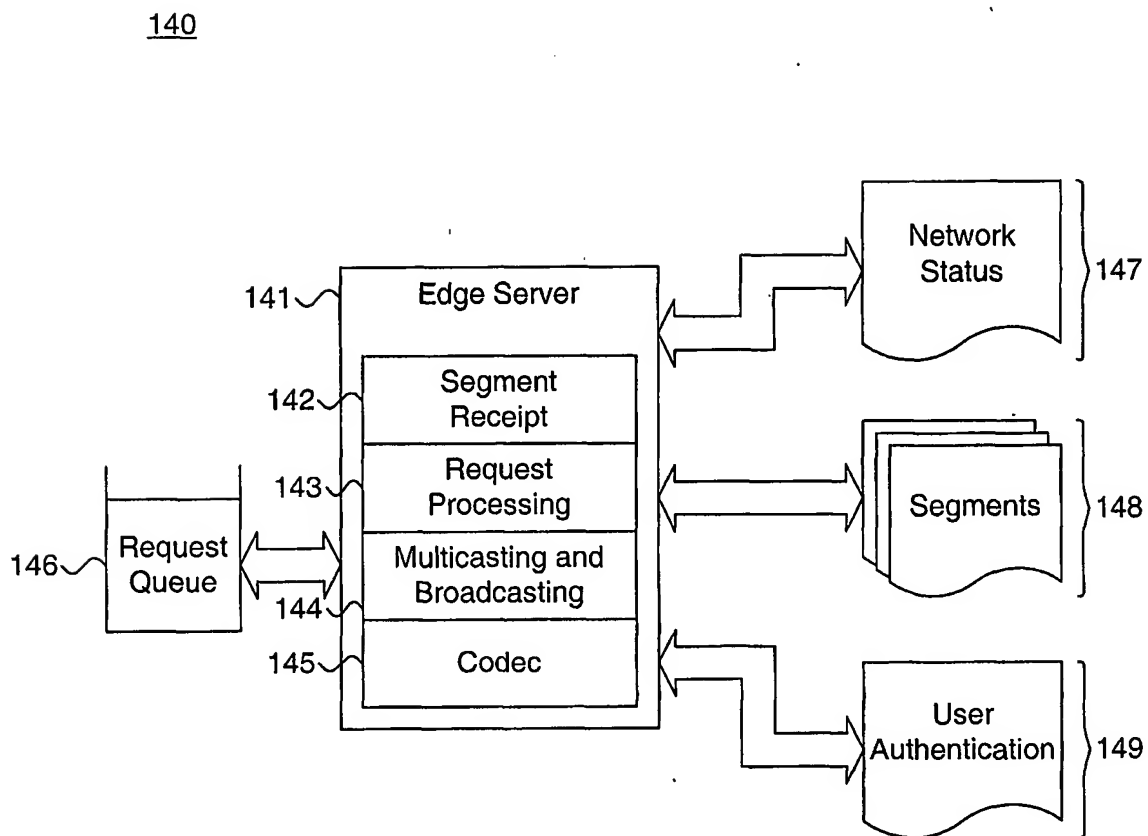
6/17

Figure 6.



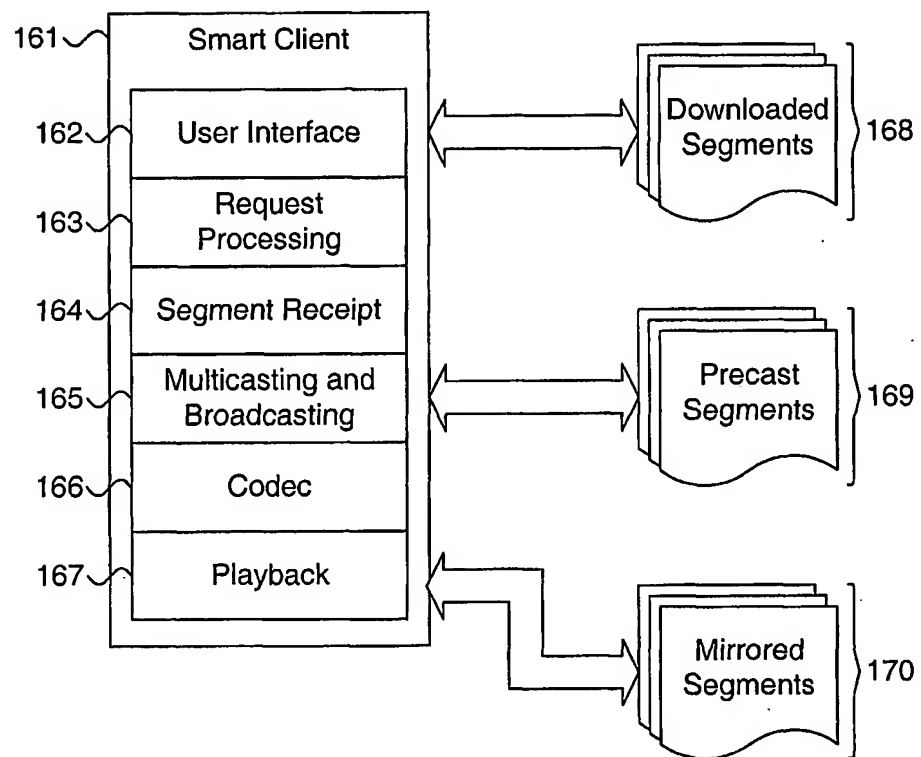
7/17

Figure 7.



8/17

Figure 8.

160

9/17

Figure 9.180

Certificate Serial No. (181)		Customer No. (182)
Create Date/Time (183)	Expire Date/Time (184)	Movie Title No. (185)
No. of Plays (186)	Reserved (187)	
Movie Key (Part I) (188)		
Certificate Signature (189)		

Figure 10.200

Certificate Serial No. (201)		Customer No. (202)
Create Date/Time (203)	Expire Date/Time (204)	Movie Title No. (205)
Reserved (206)		
Movie Key (Part 2) (207)		
Certificate Signature (208)		

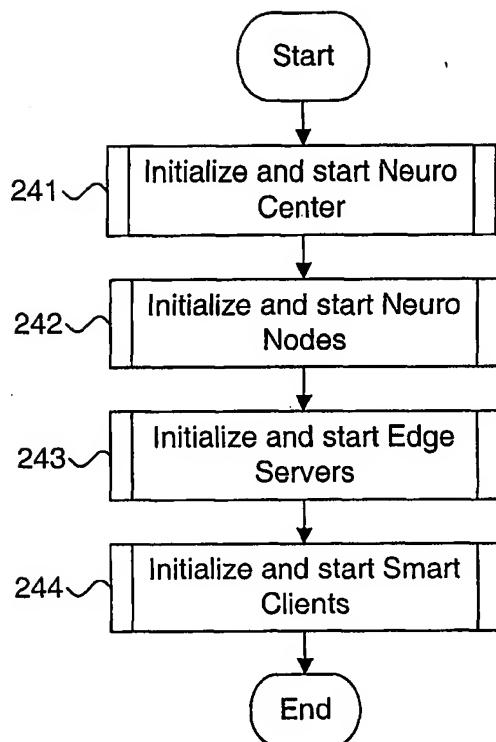
10/17

Figure 11.220

Source (221)	Destination (222)
Packet Length (223)	Checksum (224)
Type (225)	
Data Owner (226)	
Sequence No. (227)	
Header Extensions (228)	
Data (229)	

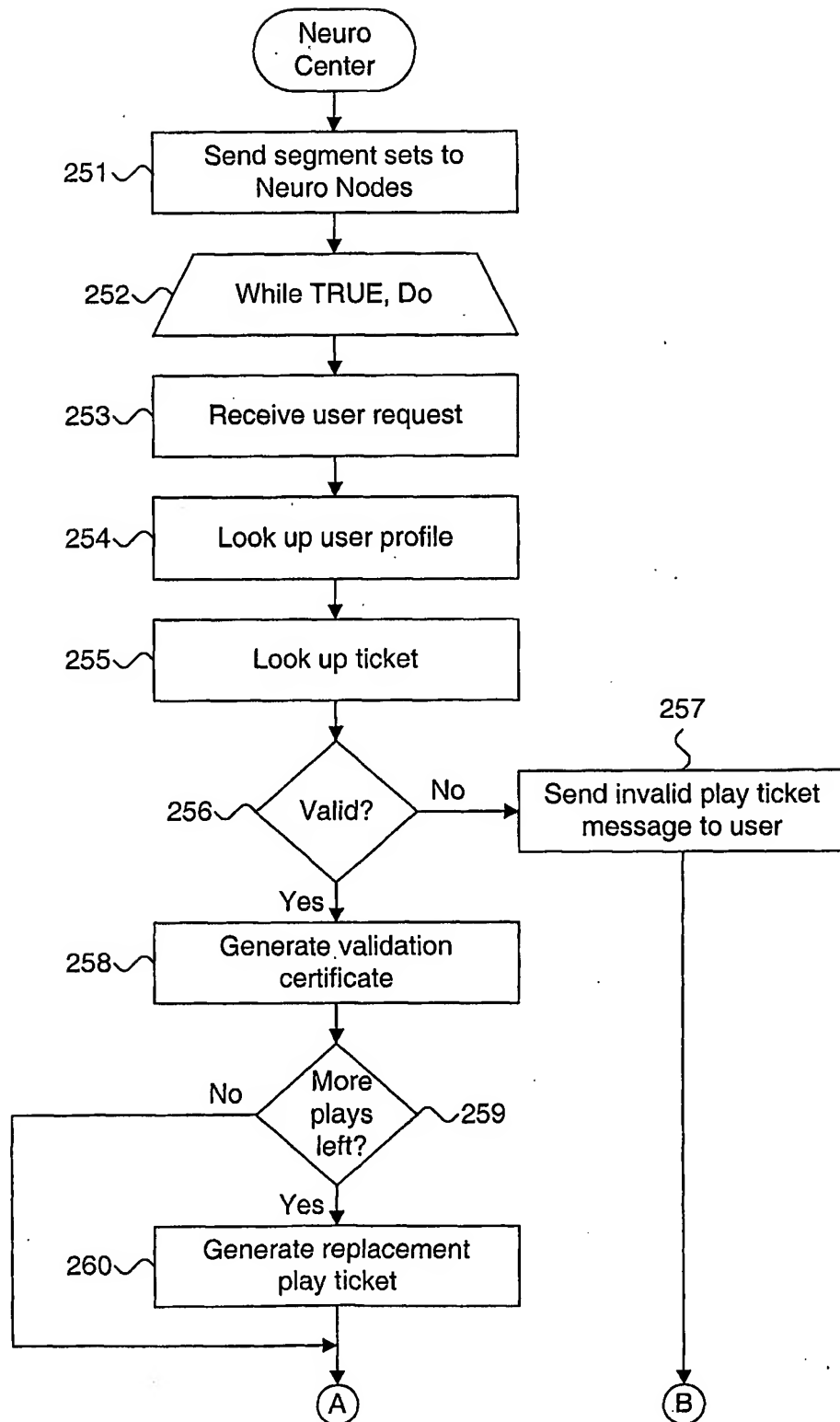
11/17

Figure 12.

240

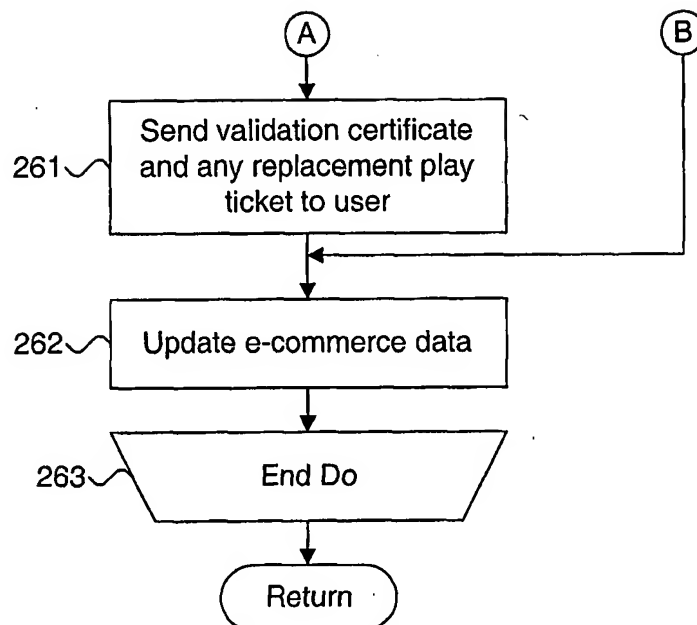
12/17

Figure 13.

250

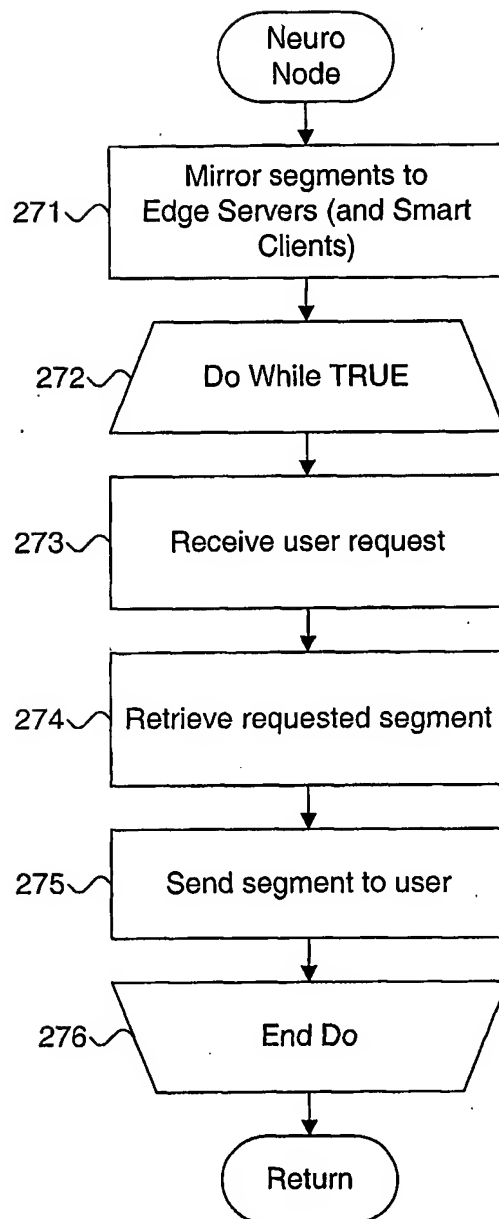
13/17

Figure 13 (cont'd).



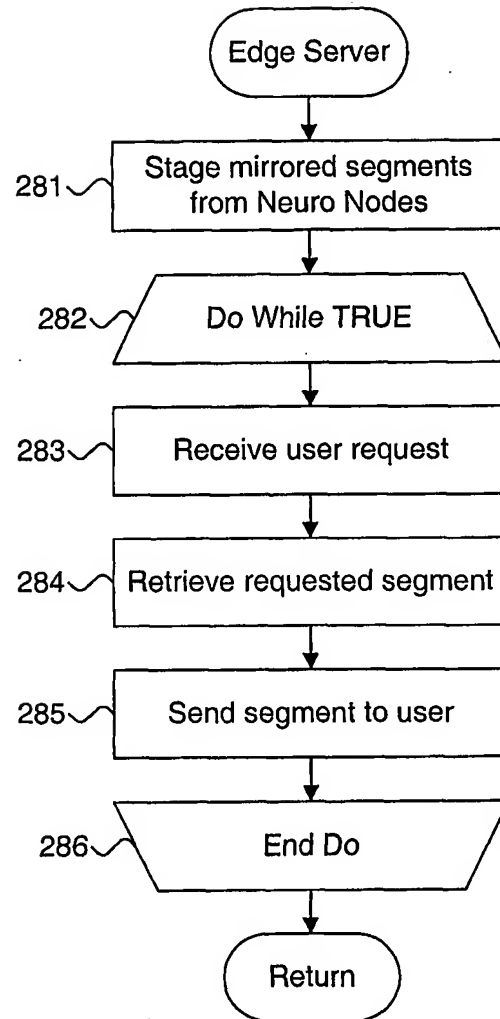
14/17

Figure 14.

270

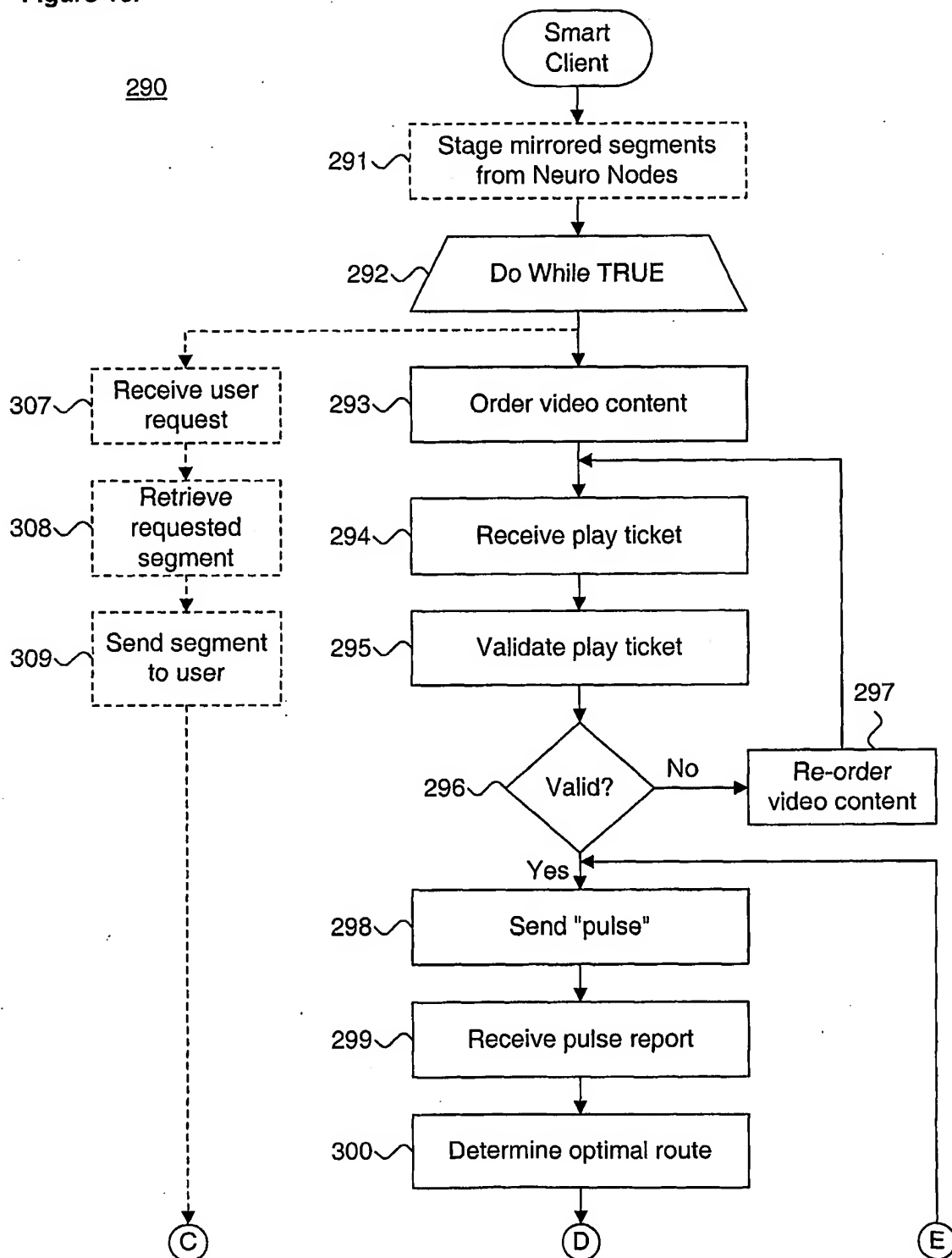
15/17

Figure 15.

280

16/17

Figure 16.



17/17

Figure 16 (cont'd).

